Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter

Studienbericht

www.bitkom.org

bitkom

Herausgeber
Bitkom e.V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner
Marc Bachmann | Bereichsleiter Öffentliche Sicherheit & Verteidigung
T 030 27576-102 | m.bachmann@bitkom.org

Projektteam
Marc Bachmann | Maurice Shahd | Franz Grimm (Bitkom Research GmbH)

Redaktion
Maurice Shahd

Gestaltung
Astrid Scheibe

Bildnachweis
- Titelbild: © Beatrix Boros – Stocksy United | Seite 5: © Liam Grant – Stocksy United | Seite 6: © Mosuno – Stocksy United
- Grafiken unter Verwendung von © sharpnose - Fotolia.com

Inhalt

Abbildungen

Vorwort

Wer die Berichterstattung zum Thema IT-Sicherheit verfolgt, kennt die Aufsehen erregenden Fälle der vergangenen Jahre wie den groß angelegten Sony-Hack oder den Diebstahl von Prominenten-Fotos aus Apples iCloud. Das Bundesamt für Sicherheit in der Informationstechnik berichtet von gezielten Angriffen auf deutsche Industrieanlagen und Produktionsnetze. In diesem Jahr sorgte der Fall des französischsprachigen Fernsehsenders »TV5 Monde« für Aufmerksamkeit. Die Angreifer haben nicht nur Webseiten und Social-Media-Profile gehackt, sondern sind tief in die Sendetechnik eingedrungen. Das hat eine neue Qualität.

Das Know-how deutscher Unternehmen ist weltweit begehrt. Interessenten sind fremde Nachrichtendienste, Wettbewerber, kriminelle Organisationen oder, wie aktuelle Beispiele zeigen, terroristische Gruppierungen. In einem intensiven globalen Wettbewerb um Märkte und die innovativsten Produkte richten sich Wirtschaftsspionage, Sabotage und Datendiebstahl verstärkt gegen technologieorientierte und innovative mittelständische Unternehmen. In den Branchen Automobilbau, Chemie und Pharma sowie Finanzdienstleistungen sind die Fallzahlen besonders hoch, wie die hier vorliegende Studie zeigt. Auf die deutsche Gesamtwirtschaft gerechnet war jedes zweite Unternehmen in den vergangenen zwei Jahren von einem Angriff betroffen. Das führt nach konservativen Berechnungen des Bitkom zu wirtschaftlichen Schäden in Höhe von rund 51 Milliarden Euro pro Jahr.

Viele Unternehmen sind sich der Risiken eines ungewollten Know-how-Verlustes nicht bewusst oder verfügen über kein wirksames Sicherheitskonzept. Auch auf die Nachsorge hat sich nur die Hälfte der Unternehmen vorbereitet. Ein gutes Notfallmanagement könnte dafür sorgen, Schäden möglichst gering zu halten und Ausfälle zu vermeiden. Prävention und Aufklärung können nur funktionieren, wenn Wirtschaftsschutz als Teamarbeit verstanden wird. Wirtschaft und Behörden sollten an einem Strang ziehen, um gemeinsam den Wirtschaftsstandort Deutschland und Europa zu schützen und unsere gute Position auf dem Weltmarkt zu verteidigen.

Mit der Studie »Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter“ wollen wir dieses Thema auf einer validen, empirisch abgesicherten Datengrundlage beleuchten, die Unternehmen sensibilisieren und die Diskussion über die Thematik versachlichen.

Dr. Bernhard Rohleder

Summary

Schäden

Die Studie hat gezeigt, dass 51 Prozent der Unternehmen in den letzten zwei Jahren von Wirtschaftsspionage, Sabotage und Datendiebstahl betroffen waren. Dabei entstand ein Schaden von 51 Milliarden Euro pro Jahr. Das entspricht 1,75 Prozent vom jährlichen BIP.

Gleichzeitig verfügen 51 Prozent der Unternehmen nicht über ein Notfallmanagement, dass es Ihnen erlaubt Schäden einzugrenzen und im Fall der Betroffenheit möglichst schnell den Betrieb wieder aufnehmen zu können oder gar nicht erst unterbrechen zu müssen.

Es handelt sich um einen Bereich mit immensen Auswirkungen auf die deutsche Wirtschaft. Deshalb ist eine gemeinsame Anstrengung von Wirtschaft, Politik und Sicherheitsbehörden notwendig. Vor diesem Hintergrund ist es bedenklich, dass sich nur jedes fünfte Unternehmen (20 Prozent) an staatliche Stellen wendet.

Sicherheit

Von den befragten Unternehmen gaben 75 Prozent an, regelmäßig von Angriffen auf Ihre IT-Systeme betroffen zu sein. Als Reaktion haben 100 Prozent technische Sicherheitsmaßnahmen ergriffen. Dazu gehören Virenscanner, Firewalls und regelmäßige Updates.

Da die Angriffe aber immer komplexer werden sind auch zusätzliche Schutzmaßnahmen notwendig. Dazu gehören zum Beispiel Verschlüsselungstechniken insbesondere für sensible Daten, aber auch neue Technologien im Bereich Intrusion Detection, Intrusion Prevention und Data Leakage Prevention.

Hier haben viele Unternehmen noch Nachholbedarf. Dafür ist bei vielen Unternehmen auch ein Umdenken notwendig, dass sich Investitionen in Sicherheit auch langfristig auszahlen und nicht nur der monetäre Aufwand im Vordergrund stehen darf.

Organisation

Auch die Organisation kann für mehr Sicherheit sorgen. Dazu gehören unter anderem Regelungen, wer im internen Netzwerk auf welche Daten zugreifen darf und wer Zutritt zu sensiblen Bereichen eines Unternehmens bekommt. Immerhin 87 Prozent der befragten Unternehmen machen sich darüber Gedanken.

Ein Notfallmanagement gewährleistet eine schnelle Reaktion im Krisenfall. Darüber verfügt bisher nur knapp die Hälfte (49 Prozent) der Unternehmen in Deutschland.

Eine Möglichkeit den Aspekt der Sicherheit innerhalb der Organisation zu erhöhen sind Sicherheitszertifizierungen. Sie zwingen das Unternehmen, sich mit dem Thema intensiv auseinanderzusetzen. In der Praxis sind sie ein geeignetes Mittel, um höhere Sicherheitsstandards im gesamten Unternehmen zu etablieren.

Faktor Mensch

Bei 52 Prozent der von Wirtschaftsspionage, Sabotage und Datendiebstahl betroffenen Unternehmen war ein aktueller oder ehemaliger Mitarbeiter das Einfallstor. Die Motive sind ganz unterschiedlich. Auch kann es sich um Fälle von Naivität handeln. So ist Social Engineering, also das Manipulieren von Mitarbeitern, mit 19 Prozent eines der häufigsten Delikte.

Demgegenüber führen nur 52 Prozent der Befragten Schulungen der Mitarbeiter oder Sicherheitsüberprüfungen von Bewerbern durch. Eine angemessene Sicherheitskultur umfasst darüber hinaus die richtige Verwendung von Zugangsdaten, den korrekten Umgang mit externen Datenträgern oder Verhaltensregeln auf Reisen.

»Digitale Angriffe sind eine reale Gefahr für Unternehmen. Viele Unternehmen schützen ihre materiellen und immateriellen Werte nicht ausreichend. Gerade der Mittelstand muss beim Thema Sicherheit nachlegen.«

Prof. Dieter Kempf auf der Pressekonferenz zu Wirtschaftsspionage,
Sabotage und Datendiebstahl am 16.04.2015 in Berlin

Jedes zweite Unternehmen ist in Deutschland von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl betroffen. Besonders betroffen sind die Automobil-, Chemie- und Pharma-Branche sowie das Finanz- und Versicherungswesen. Häufigstes Delikt ist der Diebstahl von IT- oder Telekommunikationsgeräten wie Computer, Smartphones oder Tablets und der darauf gespeicherten Daten.

1.1 Spionage, Sabotage oder Datendiebstahl trifft jedes zweite Unternehmen

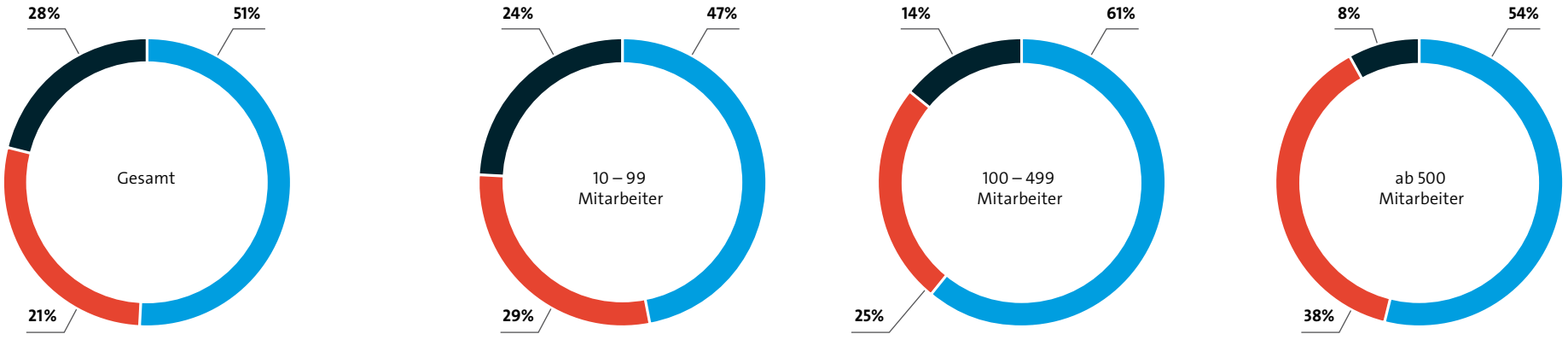
Abbildung 1: Betroffene Unternehmen nach Betriebsgrößenklassen

Basis: Alle befragten Unternehmen (n=1.074)
Quelle: Bitkom Research

Betroffen
Vermutlich betroffen
Nicht betroffen

Gut die Hälfte (51 Prozent) aller Unternehmen in Deutschland ist in den vergangenen zwei Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden. Weitere 28 Prozent geben an, dass ihr Unternehmen vermutlich betroffen ist. Am stärksten trifft es mittelständische Unternehmen, die zwischen 100 und 499 Mitarbeitern beschäftigen, mit 61 Prozent. Die großen Unternehmen ab 500 Mitarbeitern liegen etwas über dem Durchschnitt (54 Prozent) und die kleineren Betriebe mit zehn bis 99 Beschäftigten etwas darunter (47 Prozent).

Der Mittelstand ist aus mehreren Gründen ein besonders lukratives Angriffsziel. Viele Unternehmen bieten sehr innovative Produkte an und haben in ihrem Marktsegment international eine starke Stellung. Häufig sind sie als Zulieferer fest in den Lieferketten von Großkonzernen verankert. Sie verfügen aber nicht über die gleichen Mittel zur Abwehr entsprechender Angriffe und können somit als Einfallstor dienen, um an die Geschäftsgeheimnisse der Großkonzerne zu gelangen.



1.2 Industrie und Finanzwesen am stärksten betroffen

Betrachtet man die betroffenen Unternehmen differenziert nach Branchen, zeigen sich erhebliche Unterschiede: Die Automobilindustrie ist der am stärksten gefährdete Wirtschaftszweig mit 68 Prozent betroffener Unternehmen. Das ist wenig überraschend, denn die deutschen Fahrzeugbauer und ihre Zulieferer gehören zu den innovativsten Unternehmen weltweit.

Es folgen die Chemie- und Pharma-Branche mit 66 Prozent sowie das Finanz- und Versicherungswesen mit 60 Prozent. Das Gesundheitswesen und die Medien kommen auf jeweils 58 Prozent. Die IT- und Telekommunikationsindustrie rangiert im Mittelfeld mit 52 Prozent. Die besonders kritischen Energie- und Wasserversorger liegen mit 45 Prozent unter dem Schnitt. Genauso wie der Maschinen- und Anlagenbau sowie die Ernährungsindustrie (44 Prozent).

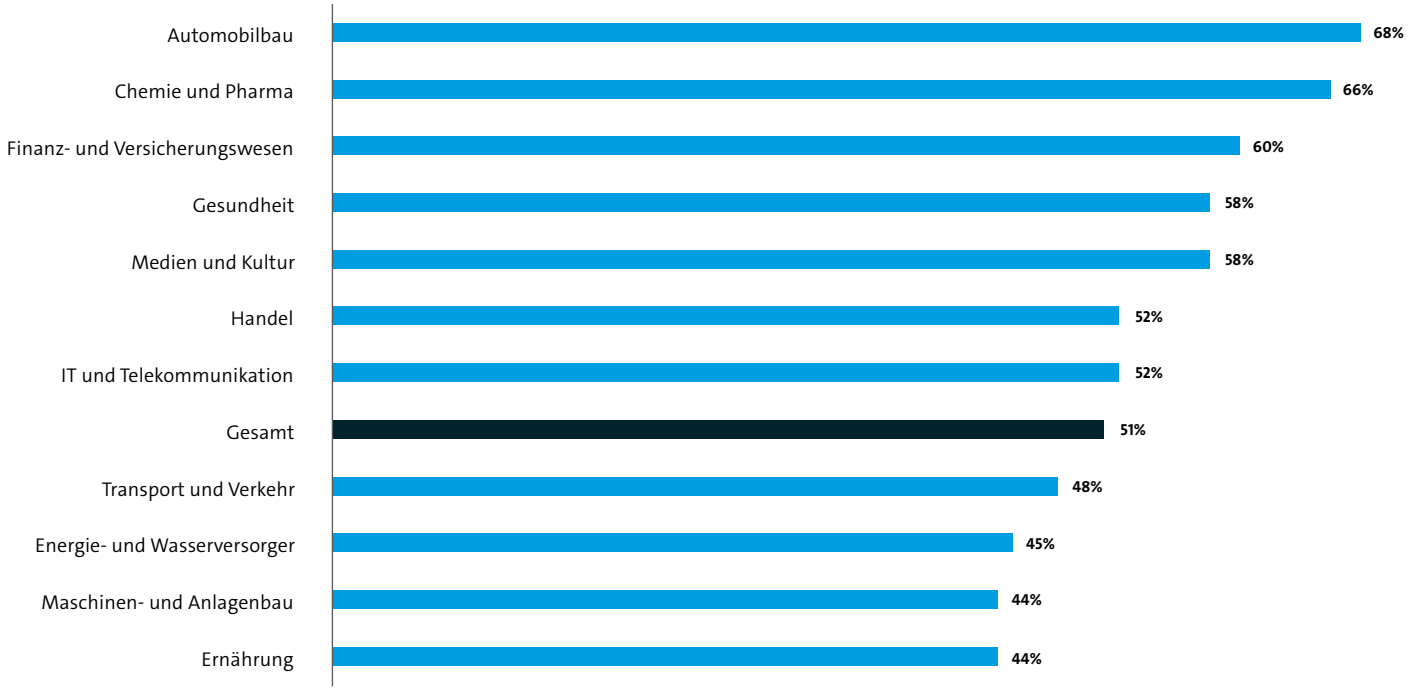


Abbildung 2: Betroffene Unternehmen nach Branchen

Basis: Alle befragten Unternehmen (n=1.074) | Quelle: Bitkom Research

1.3 Kein höheres Risiko für Betreiber Kritischer Infrastrukturen

Ein besonderes Augenmerk wurde bei der Befragung auf die Betreiber kritischer Infrastrukturen gelegt, weil sie besonders wichtig für das Funktionieren des Gemeinwesens sind. Dazu gehören Organisationen und Einrichtungen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen einträten. Neben Energie- und Wasserversorgern, dem Finanz- und Versicherungswesen und den Betreibern von Kommunikationsnetzen zählen dazu auch die Ernährungswirtschaft, das Gesundheitswesen, Medien und Kultur sowie Transport und Verkehr.

Im Ergebnis zeigt sich, dass die KRITIS-Branchen nicht stärker von den untersuchten Delikten betroffen sind als andere Wirtschaftszweige. Allerdings interessieren sich zum Teil andere Täterkreise für die Betreiber Kritischer Infrastrukturen (siehe Kapitel 3).

KRITIS

Organisationen und Einrichtungen mit wichtiger Bedeutung für das Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen einträten.

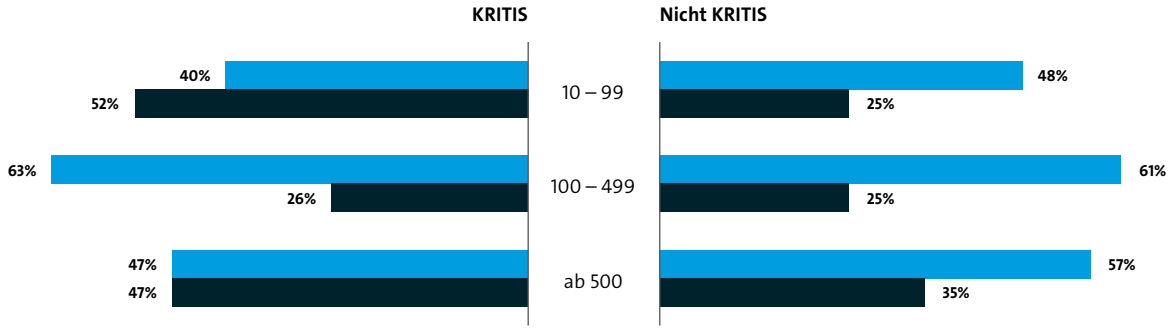


Abbildung 3: Betroffene Unternehmen nach Sektor

Basis: Alle befragten Unternehmen (n=1.074)
Quelle: Bitkom Research

Betroffen
Vermutlich betroffen

1.4 Häufigstes Delikt ist der Diebstahl von Daten und Datenträgern

Das am häufigsten auftretende Delikt ist der Diebstahl von IT- und Telekommunikationsgeräten: In 28 Prozent der befragten Unternehmen sind in den letzten zwei Jahren zum Beispiel Computer, Smartphones oder Tablets gestohlen worden. Allerdings geht daraus nicht hervor, ob es die Täter auf das Gerät oder die darauf befindlichen Informationen abgesehen haben.

Fast ein Fünftel (19 Prozent) der Unternehmen registrierte in den vergangenen zwei Jahren Fälle von Social Engineering. Bei dieser Methode geht es darum, Mitarbeiter zu manipulieren, um an bestimmte Informationen zu gelangen. Häufig geht Social Engineering gezielten Hacking- oder Phishing-Angriffen voraus. Mithilfe von Informationen aus dem Umfeld der Mitarbeiter werden dann beispielsweise täuschend echte E-Mails von vermeintlichen Bekannten verfasst, deren Anhang vom Adressaten geöffnet wird. Auf diese Weise gelangen Trojaner auf die Computer, die in der Folge Passwörter und andere Daten aushorchen.

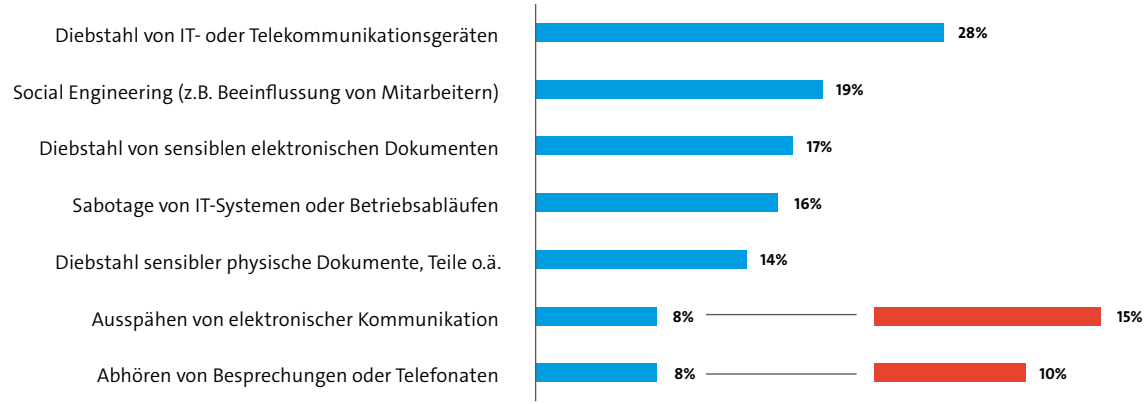
Weitere 17 Prozent der befragten Unternehmen berichten vom Diebstahl sensibler elektronischer Dokumente bzw. Daten und 16 Prozent von Sabotage ihrer IT-Systeme oder Betriebsabläufe. Der Angriff auf den französischsprachigen TV-Sender TV5 Monde war im Jahr 2015 ein typischer Fall von erfolgreicher Sabotage. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen Fall dokumentiert, bei dem in Deutschland ein Hochofen nach einem IT-Angriff schwer beschädigt wurde. Solche Vorfälle werden mit der immer stärkeren Vernetzung zunehmen.

Bei acht Prozent der Unternehmen ist die elektronische Kommunikation ausgespäht worden. Unter den großen Unternehmen ab 500 Mitarbeitern beträgt dieser Anteil sogar 15 Prozent. Das Abhören von Telefonaten oder Besprechungen gehört eher zu den selteneren Fällen der Wirtschaftsspionage. Nur acht Prozent der Unternehmen haben nach eigenen Angaben in den vergangenen zwei Jahren solche Angriffe festgestellt.

Bei immerhin 14 Prozent sind sensible physische Dokumente, Muster, Bauteile oder sogar Maschinen gestohlen worden. Zusammenfassend zeigt sich, dass nahezu alle Fälle von Sabotage oder Spionage im wirtschaftlichen Umfeld heute auf digitale Daten oder die Informations- und Kommunikationsinfrastruktur der Unternehmen abzielen. Das ist eine direkte Folge der inzwischen weit fortgeschrittenen Digitalisierung in der Wirtschaft.

Abbildung 4: Aufgetretene Delikte

Basis: Alle befragten Unternehmen (n=1.074)
Quelle: Bitkom Research



1.5 IT-Angriffe gehören zum Alltag vieler Unternehmen

Drei von vier Unternehmen sind in unterschiedlicher Intensität IT-Angriffen ausgesetzt. Bei einem IT-Angriff handelt es sich meist um den Versuch, über das Internet in die IT-Systeme einer Organisation einzudringen. Der Angriff kann aber auch über einen infizierten USB-Stick oder andere Datenträger ausgelöst werden. Ziel der Angreifer ist es, entweder Informationen zu entwenden oder die betriebsinternen Abläufe zu sabotieren.

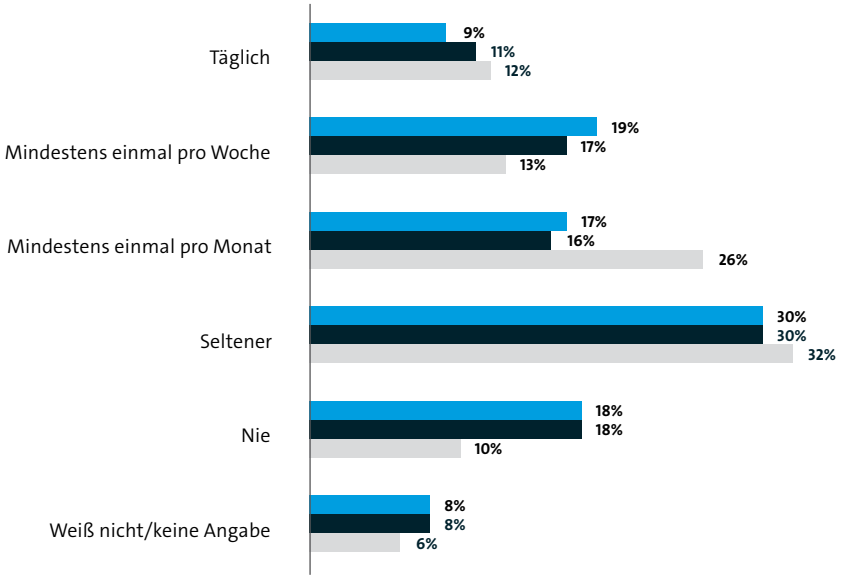


Abbildung 5: Häufigkeit von IT-Angriffen

Basis: Alle befragten Unternehmen (n=1.074)
Quelle: Bitkom Research

IT-Angriffe sind in der Regel die Grundlage für Datendiebstahl oder Sabotageakte. Nahezu die Hälfte (45 Prozent) wird regelmäßig angegriffen, also mindestens einmal pro Monat, fast jedes zehnte Unternehmen (9 Prozent) sogar täglich. Je größer die Unternehmen sind, desto häufiger werden sie auf diese Weise attackiert.

Der Großteil der Angriffe wird von Firewall oder Virenscanner abgewehrt. Auf der anderen Seite bleiben viele Angriffe unentdeckt. Manche Schadsoftware ist so raffiniert programmiert, dass sie von normalen Virenscannern nicht mehr erkannt wird. Der Grundschutz, der in der Regel in den gängigen Betriebssystemen integriert ist, reicht in vielen Fällen nicht mehr aus (siehe Kapitel 5).

1.6 Die IT ist das zentrale Angriffsziel

Häufigstes Angriffsziel sind die IT-Systeme und die Kommunikationsinfrastruktur der Unternehmen. Sie sind das Einfallstor für digitale Spionage- und Sabotageakte. Es folgen die Bereiche Lager und Logistik, der Einkauf, die Produktion sowie die Geschäftsleitung.

Dass der Bereich Forschung und Entwicklung mit neun Prozent das Schlusslicht bildet, überrascht nur auf den ersten Blick. Die meisten kleinen Unternehmen, die den Großteil der Befragten ausmachen, haben gar keine eigenen Forschungs- und Entwicklungsabteilungen. Dagegen geben fast ein Drittel (30 Prozent) der großen Unternehmen ab 500 Mitarbeitern an, dass ihre F&E-Bereiche gehackt oder ausspioniert worden sind.

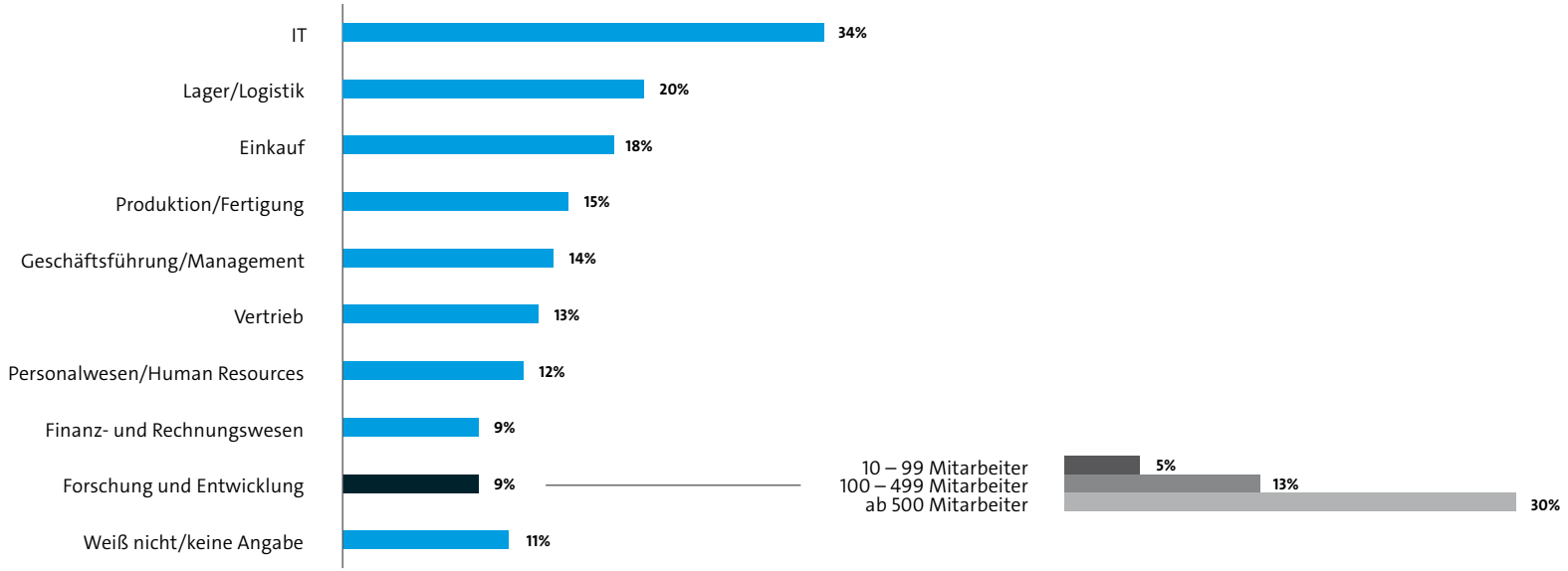


Abbildung 6: Betroffene Unternehmensbereiche

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Wirtschaftsspionage oder Sabotage betroffen waren (n=550)
Quelle: Bitkom Research

2 Aufgetretene Schäden

»Zu den Top-Schadensfällen gehören Plagiate, bei denen Informationen durch Wirtschaftsspionage abhanden gekommen sind und die dann zum Beispiel in China schneller und kostengünstiger auf den Markt kommen.«

Marc Bachmann am 19.04.2015 bei nano in 3sat

Nach konservativen Berechnungen beläuft sich der entstandene Schaden für die gesamte deutsche Wirtschaft auf rund 51 Milliarden Euro pro Jahr. Der größte Teil davon geht auf Umsatzeinbußen durch Plagiate und Patentrechtsverletzungen zurück.

2.1 Schadenberechnungsmodell

Ein zentrales Ziel dieser Studie bestand darin, den Gesamtschaden für die deutsche Wirtschaft zu bestimmen, der durch Wirtschaftsspionage, Sabotage oder Datendiebstahl entsteht. Dementsprechend wurde der Fragebogen und die Vorgehensweise gestaltet.

Allen befragten Unternehmen wurde der Fragebogen vor dem Telefoninterview zur Verfügung gestellt. Zu Beginn der telefonischen Befragung wurden die Unternehmen gefragt, von welchen Handlungen diese innerhalb der letzten zwei Jahre betroffen waren. Dann wurden sie gefragt, welche Schäden daraus entstanden sind. In einem weiteren Schritt wurden dann die Schadenssummen für die einzelnen Delikte abgefragt, die genannten Summen während des Telefoninterviews aufaddiert und dem Befragten bei der abschließenden Frage nach dem Gesamtschaden genannt. Damit hatte jeder Befragte die Möglichkeit, die Teilschadenssummen sowie die Summe des Gesamtschadens abschließend zu verifizieren.

Schließlich wurden die durchschnittlichen Schadenssummen für die einzelnen Delikte auf die deutsche Gesamtwirtschaft hochgerechnet. Bei der Berechnung der Durchschnittswerte bzw. Mittelwerte wurde das sogenannte »fünf Prozent getrimmte Mittel« verwendet. Hierbei werden 2,5 Prozent der kleinsten und 2,5 Prozent der größten Werte ausgeblendet und der Mittelwert über die verbleibenden Werte berechnet. Die durchschnittlichen Schadenssummen sind somit um Ausreißer nach oben und unten bereinigt. Folglich kann man von einer konservativen Berechnung der Schadenssummen sprechen. Die Hochrechnung erfolgte auf der Grundlage der Umsatzsteuerstatistik des Statistischen Bundesamtes, die aktuell rund 355.000 Unternehmen ab zehn Mitarbeitern ausweist. Basis für die Hochrechnung sind alle betroffenen Unternehmen mit einem nachweislichen finanziellen Schaden. Das sind 48 Prozent der befragten Unternehmen und entspricht rund 170.000 Unternehmen.

2.2 Pro Jahr 51 Milliarden Euro Schaden

Der Schaden als Folge digitaler Wirtschaftsspionage, Sabotage und Datendiebstahl liegt nach konservativen Berechnungen bei rund 51 Milliarden Euro pro Jahr. Fast ein Viertel dieser Summe und damit der größte Teil geht auf Umsatzverluste durch Plagiate zurück. Es folgen Patentrechtsverletzungen, die ähnliche Folgen wie Plagiate haben. An dritter Stelle liegen Umsatzeinbußen durch den Verlust von Wettbewerbsvorteilen. Das kann zum Beispiel der Vorsprung bei der Einführung neuer Produkte sein, der es Unternehmen erlaubt, höhere Preise zu verlangen und damit die Entwicklungskosten zu amortisieren.

Ein weiterer großer Posten sind Kosten infolge des Diebstahls von ITK-Geräten sowie Ausgaben, die durch den Ausfall von IT-Systemen oder die Störung von Betriebsabläufen entstehen. Ein weicher Faktor mit großem Gewicht sind Imageschäden, die nach Sicherheitsvorfällen eintreten. Gelten ein Unternehmen oder seine Produkte bei Kunden und Geschäftspartnern erst einmal als unsicher, ist das nur schwer aus der Welt zu schaffen. Ein solcher Reputationsverlust kann im schlimmsten Fall ein Unternehmen in seiner Existenz gefährden. Hohe Kosten verursachen außerdem Rechtsstreitigkeiten.

Delikttyp	Schadenssumme (in Euro)
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	23,0 Mrd.
Patentrechtsverletzungen (auch vor der Anmeldung)	18,8 Mrd.
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	14,3 Mrd.
Ausfall, Diebstahl oder Schädigung von IT-Systemen, Produktions- oder Betriebsabläufen	13,0 Mrd.
Imageschaden bei Kunden oder Lieferanten / Negative Medienberichterstattung	12,8 Mrd.
Kosten für Rechtsstreitigkeiten	11,8 Mrd.
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	3,9 Mrd.
Erpressung mit gestohlenen Daten	2,9 Mrd.
Höhere Mitarbeiterfluktuation / Abwerben von Mitarbeitern	1,7 Mrd.
Sonstige Schäden	0,2 Mrd.
Gesamtschaden innerhalb der letzten zwei Jahre	**102,4 Mrd.**

Abbildung 7: Aufgetretene Schäden nach Delikttyp

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Wirtschaftsspionage oder Sabotage betroffen waren (n=550)
Quelle: Bitkom Research

»Oftmals sind eigene oder ehemalige Mitarbeiter das Einfallstor. Dies kann aus Unvorsichtigkeit, aber auch aus Mutwilligkeit passieren.«

Marc Bachmann in »Computer und Kommunikation«
am 18.04.2015, Deutschlandfunk

Ausgangspunkt für Spionage, Sabotage und Datendiebstahl ist in der Regel das enge unternehmerische Umfeld. Dazu gehören in erster Linie die eigenen Beschäftigten oder ehemalige Mitarbeiter. Aber auch Kunden, Lieferanten, Dienstleister und natürlich die direkten Wettbewerber sind für Angriffe verantwortlich.

3.1 Mitarbeiter werden zu Tätern

Der mit Abstand wichtigste Täterkreis sind aktuelle oder ehemalige Mitarbeiter. Gut die Hälfte (52 Prozent) der betroffenen Unternehmen gibt diesen Personenkreis als Täter an. Das passt zu den Erkenntnissen zum Social Engineering. Nicht immer erfolgen die Taten mit böser Absicht. Vielmehr sind Unvorsichtigkeit, Unbedarftheit und Unwissen die größten Probleme. Mit diesem Wissen können Unternehmen bei den eigenen Mitarbeitern ansetzen, um die personelle Sicherheit zu erhöhen. Die zweite große Tätergruppe mit 39 Prozent umfasst das direkte unternehmerische Umfeld, bestehend aus Wettbewerbern, Lieferanten, Dienstleistern und Kunden. Dienstleister, Lieferanten und Kunden haben in vielen Fällen direkten Zugang zu einer Organisation und kennen sich mit den Gegebenheiten aus. Das erleichtert es den Tätern, einen Angriff auszuführen. 17 Prozent nennen Hobby-Hacker als Täter. Elf Prozent sind Opfer organisierter Bandenkriminalität geworden und drei Prozent standen im Visier ausländischer Geheimdienste. Bei 18 Prozent ist der Täterkreis unbekannt.

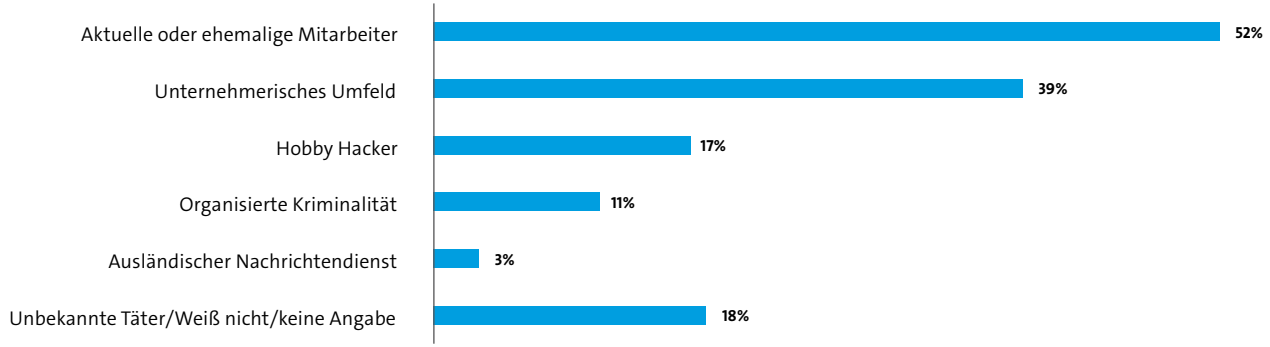


Abbildung 8: Täterkreis

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Wirtschaftsspionage oder Sabotage betroffen waren (n=550)
Quelle: Bitkom Research

3.2 China und Russland haben es auf KRITIS abgesehen

Unterschiede sind auch beim regionalen Ursprung der Taten erkennbar. Handlungen aus Deutschland und aus dem Ausland sind etwa gleich verteilt. Hinter Deutschland sortieren sich Japan, Osteuropa, USA und Russland ein. Fast ein Viertel (23 Prozent) kann keine Angaben zum Ursprung der Attacken machen.

Betrachtet man die KRITIS-Sektoren isoliert, so stammen die Täter bei den Betreibern Kritischer Infrastrukturen deutlich häufiger aus Russland, den USA, Westeuropa und China. Dagegen liegen bei allen anderen Branchen Japan und Osteuropa – hinter Deutschland – ganz vorne. Die hohe Prozentzahl für Deutschland ist wiederum ein Dunkelfeld. Denn es bleibt letztendlich unklar, wer die wahren Urheber sind.

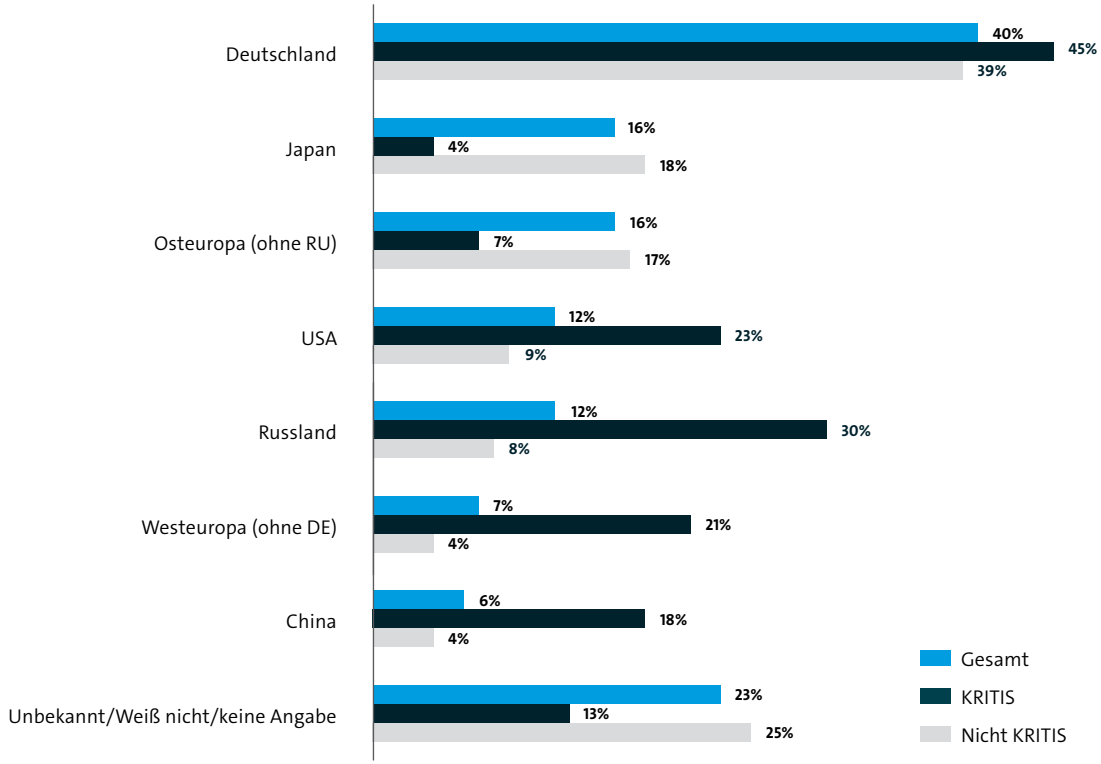


Abbildung 9: Länder und Regionen aus denen Angriffe vorgenommen werden nach KRITIS-Sektoren

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Wirtschaftsspionage oder Sabotage betroffen waren (n=550)
Quelle: Bitkom Research

4 Aufklärung

»Wir plädieren dafür, dass sich die Unternehmen an die Behörden wenden. Es gibt spezielle Dezernate, die sich um solche Fälle kümmern.«

Prof. Dieter Kempf auf der Pressekonferenz zu Wirtschaftsspionage,
Sabotage und Datendiebstahl am 16.04.2015 in Berlin

Viele Unternehmen verlassen sich auf interne Untersuchungen, um Angriffe im Bereich Wirtschaftsspionage, Sabotage und Datendiebstahl aufzuklären. An zweiter Stelle folgen externe Spezialisten und erst an dritter Stelle staatliche Institutionen. Vor allem die Angst vor negativen Konsequenzen hält die Unternehmen davon ab, sich an die Behörden zu wenden. Die Unternehmen vertrauen am ehesten der Polizei, gefolgt von Staatsanwaltschaft und BSI.

4.1 Nur jeder fünfte Betroffene wendet sich an staatliche Stellen

Mit 53 Prozent der Betroffenen hat die Mehrheit der Unternehmen eine interne Untersuchung der Vorfälle durchgeführt. Fast ein Drittel (30 Prozent) hat externe Spezialisten hinzugezogen. Dagegen hat nur jedes fünfte betroffene Unternehmen staatliche Stellen eingeschaltet. Jedes zehnte Unternehmen gibt an, gar nichts unternommen zu haben. Ein Grund dafür kann sein, dass der Vorfall als zu unwichtig eingestuft wurde.
Die niedrige Zahl derer, die sich an staatliche Stellen wenden, ist ein Problem. Ermittlungsbehörden können nur dann erfolgreich arbeiten, wenn Sie auch Kenntnis von Delikten haben. Zwar ist es für Unternehmen möglich, den Schaden aus eigener Kraft oder mit Unterstützung von Spezialisten einzudämmen. Aber nur durch die Zusammenarbeit mit staatlichen Stellen können Täter überführt und so zukünftige Delikte verhindert werden.

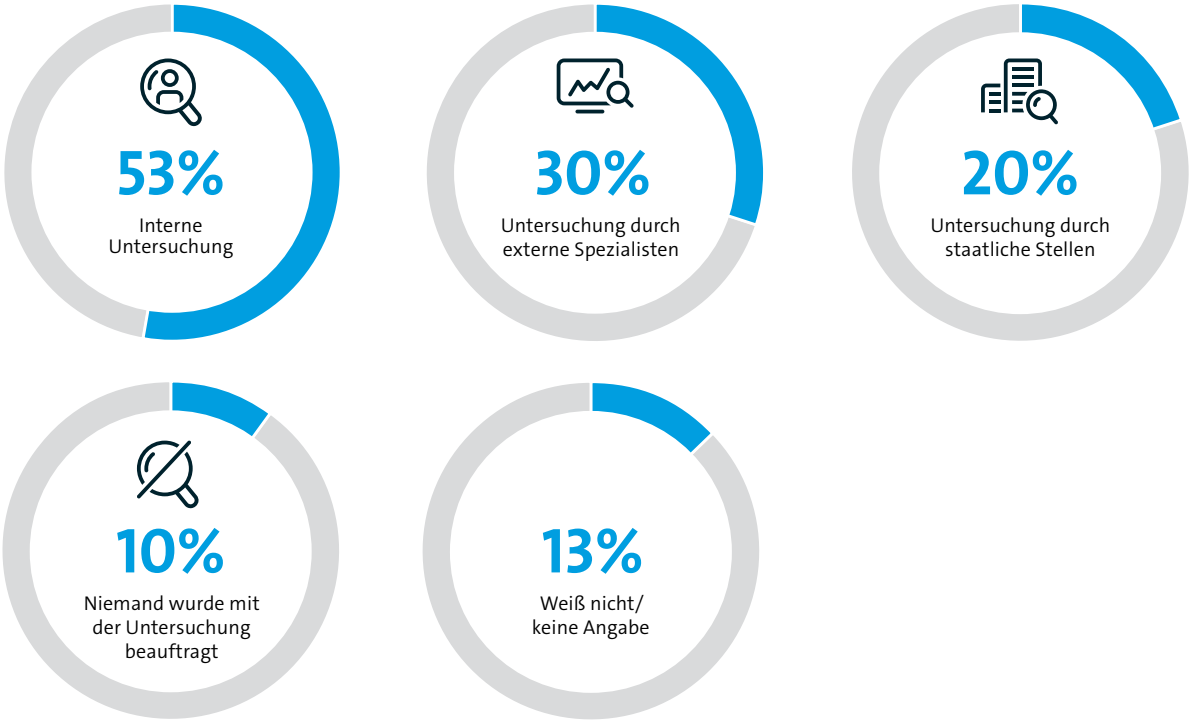


Abbildung 10: Untersuchung der Vorfälle

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Wirtschaftsspionage oder Sabotage betroffen waren (n=550)
Quelle: Bitkom Research

4.2 Unternehmen wenden sich am ehesten an die Polizei

Von den wenigen, die mit den Behörden kooperieren, wenden sich die meisten (88 Prozent) an die Polizei. Mit deutlichem Abstand folgt die Staatsanwaltschaft (46 Prozent) und das BSI (8 Prozent). Nur ein Prozent schaltet den Verfassungsschutz ein. Allerdings sind es die Verfassungsschutzbehörden der Länder und des Bundes, die in Deutschland für den Wirtschaftsschutz zuständig sind. Fraglich ist, ob die Verantwortlichen in den Unternehmen diese Zuständigkeit überhaupt kennen.
Es ist also neben der besseren Aufklärungsarbeit der einzelnen Organisationen über das eigene Aufgabengebiet auch eine gute Abstimmung zwischen den Behörden notwendig, um effektiv gegen die Angreifer vorgehen zu können.

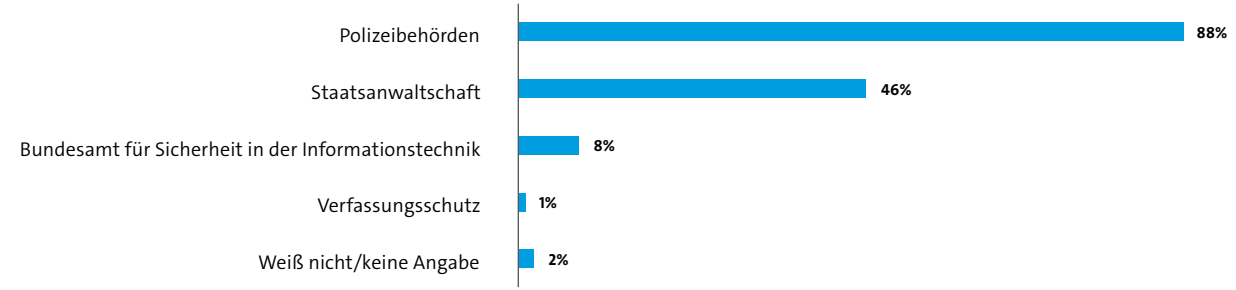


Abbildung 11: Eingeschaltete staatliche Stellen

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Wirtschaftsspionage oder Sabotage betroffen waren und staatliche Stellen bei der Untersuchung eingeschaltet haben (n=110)

Mehrfachnennungen möglich | Quelle: Bitkom Research

4.3 Angst vor negativen Konsequenzen

Was sind die Gründe, dass weder die Polizei noch anderen staatliche Stellen eingeschaltet werden? Gut ein Drittel derjenigen, die keine staatlichen Stellen informiert haben, nennt als Grund »Angst vor negativen Konsequenzen«. Das kann zum Beispiel die Sicherung von Beweismitteln wie Computern sein. Im Extremfall ist das Unternehmen dann nicht mehr arbeitsfähig.
31 Prozent nennen den hohen Aufwand als Grund. So müssen die betroffenen Unternehmen die Ereignisse dokumentieren und die Ermittler bei ihrer Arbeit unterstützen. Fast ein Viertel (23 Prozent) hat Sorge vor einem Imageschaden, wenn die Vorfälle öffentlich werden. Ebenso viele sind der Meinung, die Täter würden ohnehin nicht gefasst.

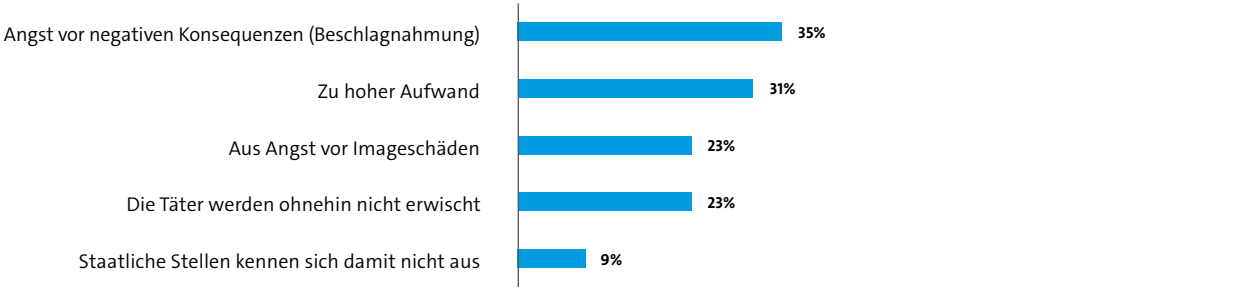


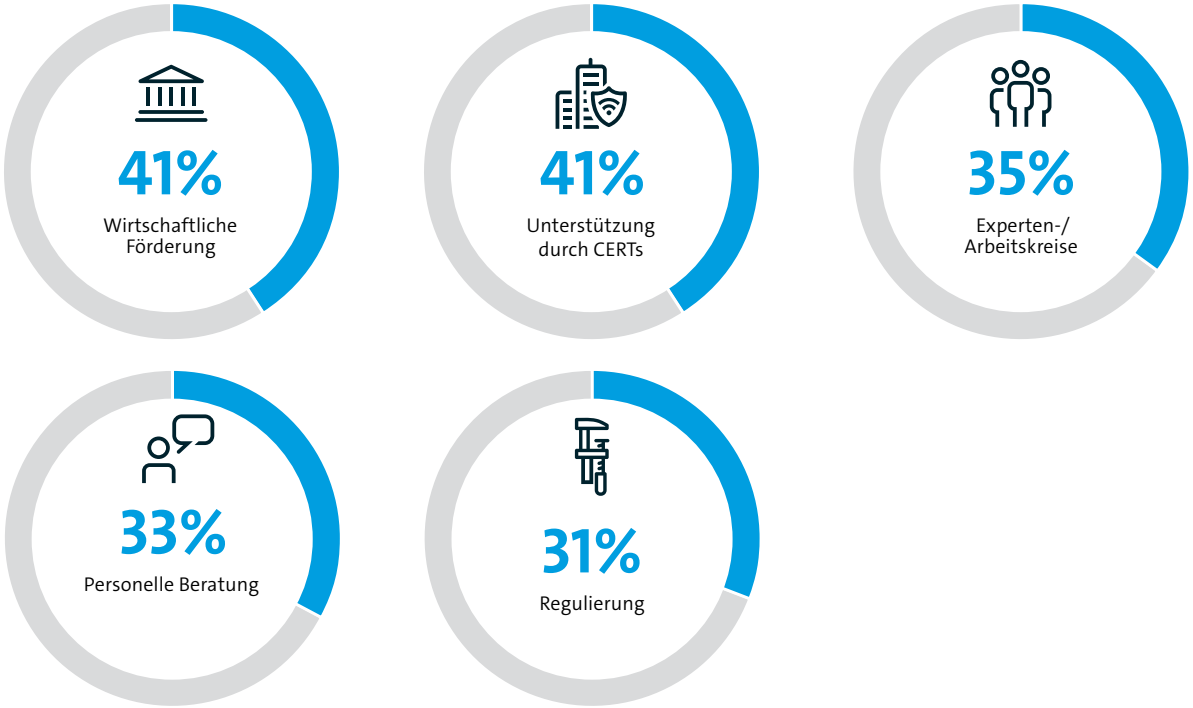
Abbildung 12: Gründe für das Nicht-Einschalten von staatlichen Stellen

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Wirtschaftsspionage oder Sabotage betroffen waren und keine staatliche Stellen bei der Untersuchung eingeschaltet haben (n=440)

Mehrfachnennungen möglich | Quelle: Bitkom Research

4.4 Forderungen an den Staat

Welche Maßnahmen kann der Staat ergreifen? Klar ist, dass die Verantwortung für die eigenen Unternehmenswerte bei den Unternehmen selbst liegt. Jedoch kann der Staat in bestimmten Bereichen den Unternehmen unterstützend zur Seite stehen. Jeweils 41 Prozent der Befragten antworteten »Wirtschaftliche Förderung« und »Unterstützung durch CERTs«.



Gerade für kleine und mittlere Unternehmen kann diese Unterstützung von herausragender Bedeutung sein, da die Ressourcen oftmals fehlen. Mit einer gezielten Förderung kann das Sicherheitsniveau beim Rückgrat der deutschen Wirtschaft nachhaltig gesteigert werden. Ähnlich verhält es sich bei den CERTs (Computer Emergency Response Teams). CERTS sind Computer-Notfallteams für präventive und reaktive Maßnahmen in Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle in Computersystemen, wie z.B. CERT-Bund. Kleine und mittlere Unternehmen verfügen nicht über eigene CERTs und wünschen sich Hilfe. Diese könnten zum Beispiel über staatlich geförderte Dienstleistungen zur Verfügung gestellt werden. Es wäre zu hoffen, dass sich an dieser Stelle die Zusammenarbeit von staatlichen Organisationen und Wirtschaft verbessern lässt.

35 Prozent der Befragten wären bereit, in Experten- bzw. Arbeitskreisen mitzuarbeiten und hier ihre Erfahrungen einzubringen. Dieses Potenzial sollte stärker genutzt werden und auch die personelle Beratung kann die Möglichkeiten eröffnen, gerade im Bereich der Prävention schon frühzeitig eine Erhöhung des Schutzniveaus zu erreichen.

Immerhin 31 Prozent wünschen sich eine stärkere Regulierung. Gesetzgeberisch einzugreifen kann eine Lösung sein, aber auch hier ist der Erfolg von einer vertrauensvollen Zusammenarbeit zwischen staatlichen Stellen und Unternehmen abhängig .

Abbildung 13: Forderungen der Wirtschaft an den Staat zum Thema Wirtschaftsschutz

Basis: Alle befragten Unternehmen (n=1.074)
Quelle: Bitkom Research

5 Sicherheitsvorkehrungen

»Nur jedes zweite Unternehmen verfügt über einen Notfallplan.«

Marc Fliehe bei »Redezeit« im NDR, am 15.04.2015

Die Unternehmen haben im Bereich der Prävention in den letzten Jahren einiges getan. So sagen alle befragten Unternehmen, dass sie über einen technischen Basisschutz vor Cyberangriffen verfügen. Allerdings ist das nicht genug. Zum einen sind weitere Maßnahmen bei der Angriffserkennung notwendig. Zum anderen sollten sich Organisationen für den Fall den Fälle vorbereiten. Bisher verfügt nur jedes zweite Unternehmen über ein Notfallmanagement.

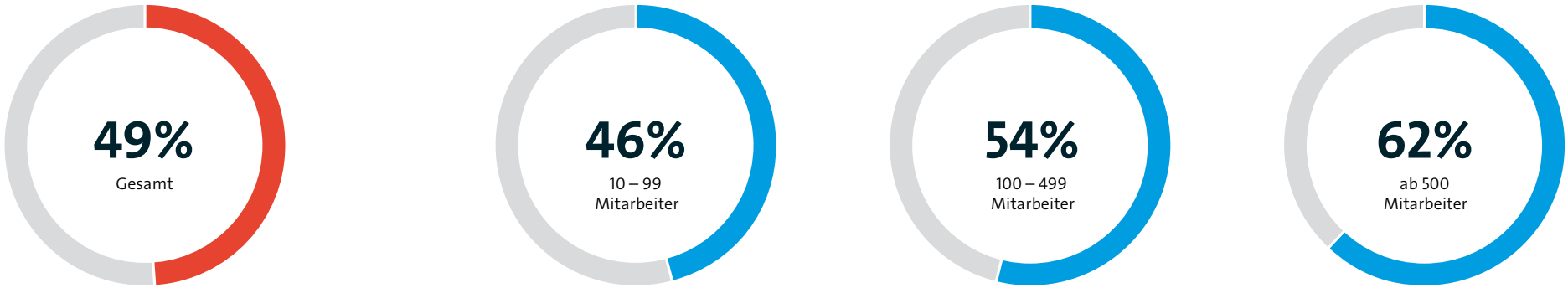
5.1 Nur die Hälfte hat ein Notfallmanagement

Nur knapp die Hälfte (49 Prozent) aller Unternehmen in Deutschland verfügt über ein Notfallmanagement bei digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl.
Größere Unternehmen sind nur unwesentlich besser gerüstet als kleinere. Bei Betrieben mit 500 oder mehr Mitarbeitern besitzen 62 Prozent ein Notfallmanagement. Bei mittelständischen Unternehmen mit 100 bis 499 Mitarbeitern sind es 54 Prozent und bei kleineren Betrieben mit 10 bis 99 Beschäftigten 46 Prozent.

Ein betriebliches Notfallmanagement umfasst schriftlich geregelte Abläufe und Sofortmaßnahmen für Situationen, in denen zum Beispiel sensible Unternehmensdaten abfließen, wichtige Webseiten wie Shops oder Online-Dienste nicht erreichbar sind oder die Produktion aufgrund digitaler Angriffe beeinträchtigt ist.
Zu den Zielen des Notfallmanagements gehört es zum Beispiel, einen Datenabfluss zu stoppen oder beim Ausfall wichtiger Systeme die Arbeitsfähigkeit des Unternehmens so schnell wie möglich wieder herzustellen.

Abbildung 14: Notfallmanagement

Basis: Alle befragten Unternehmen (n=1.074)
Quelle: Bitkom Research



5.2 Ein bisschen Sicherheit ist immer

Über Sicherheitsmaßnahmen in der einen oder anderen Form verfügen alle befragten Unternehmen. Flächendeckend setzen die Unternehmen technische IT-Sicherheitsvorkehrungen ein. Dazu zählen zum Beispiel Virenscanner und Firewalls. Allerdings reichen diese in vielen Fällen nicht mehr aus (siehe Kapitel 5.3).

Neun von zehn Unternehmen (87 Prozent) ergreifen organisatorische Sicherheitsmaßnahmen. Dazu gehören zum Beispiel Verhaltensrichtlinien für die Nutzung von Datenträgern oder Notfallpläne für Cyberangriffe. 86 Prozent sorgen für den physischen Schutz, zum Beispiel in Form von Zutrittskontrollen oder Sicherung von Gebäuden. Maßnahmen der so genannten personellen Sicherheit ergreift nur die Hälfte (52 Prozent) der Unternehmen. Und das, obwohl die meisten Täter aktuelle oder ehemalige Mitarbeiter sind. In der Praxis zählen dazu zum Beispiel Schulungen, aber auch Sicherheitsüberprüfungen von Mitarbeitern oder Bewerbern.

Ein Sonderfall sind Sicherheitszertifizierungen, die 40 Prozent der Befragten durchführen. Im Rahmen einer Zertifizierung lassen die Unternehmen ihr Sicherheitskonzept von einer externen Organisation wie dem TÜV oder dem BSI überprüfen.

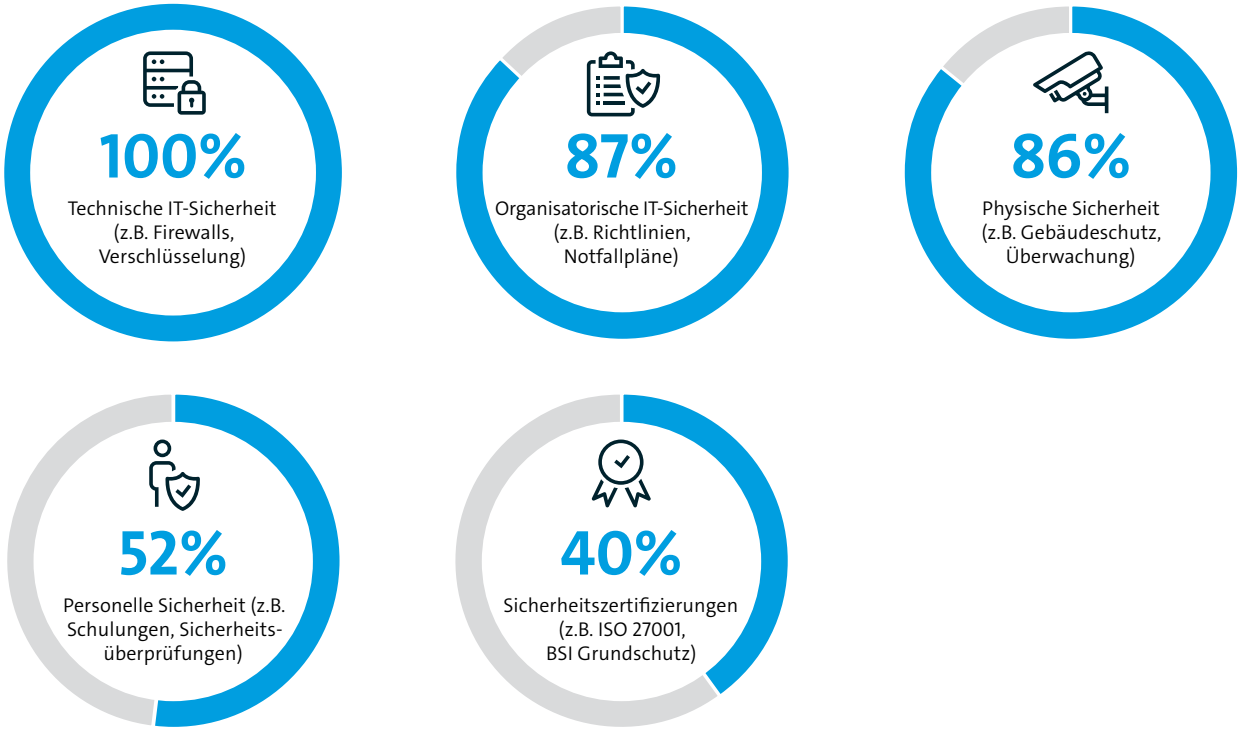


Abbildung 15: Eingesetzte Sicherheitsmaßnahmen

Basis: Alle befragten Unternehmen (n=1.074)
Quelle: Bitkom Research

5.3 Technische Sicherheitsmaßnahmen

Die Unternehmen in Deutschland verfügen bei der Absicherung ihrer IT-Systeme vor Cyberangriffen über einen guten Basisschutz, investieren aber noch zu selten in umfassende Sicherheitsmaßnahmen. So nutzen alle befragten Unternehmen Virenscanner, Firewalls sowie einen Passwortschutz für Computer und andere Kommunikationsgeräte. Diese Funktionen sind in der Regel in den gängigen Betriebssystemen enthalten, reichen aber häufig nicht mehr aus. Die Schadsoftware wird immer komplexer und bleibt nicht selten unerkannt.

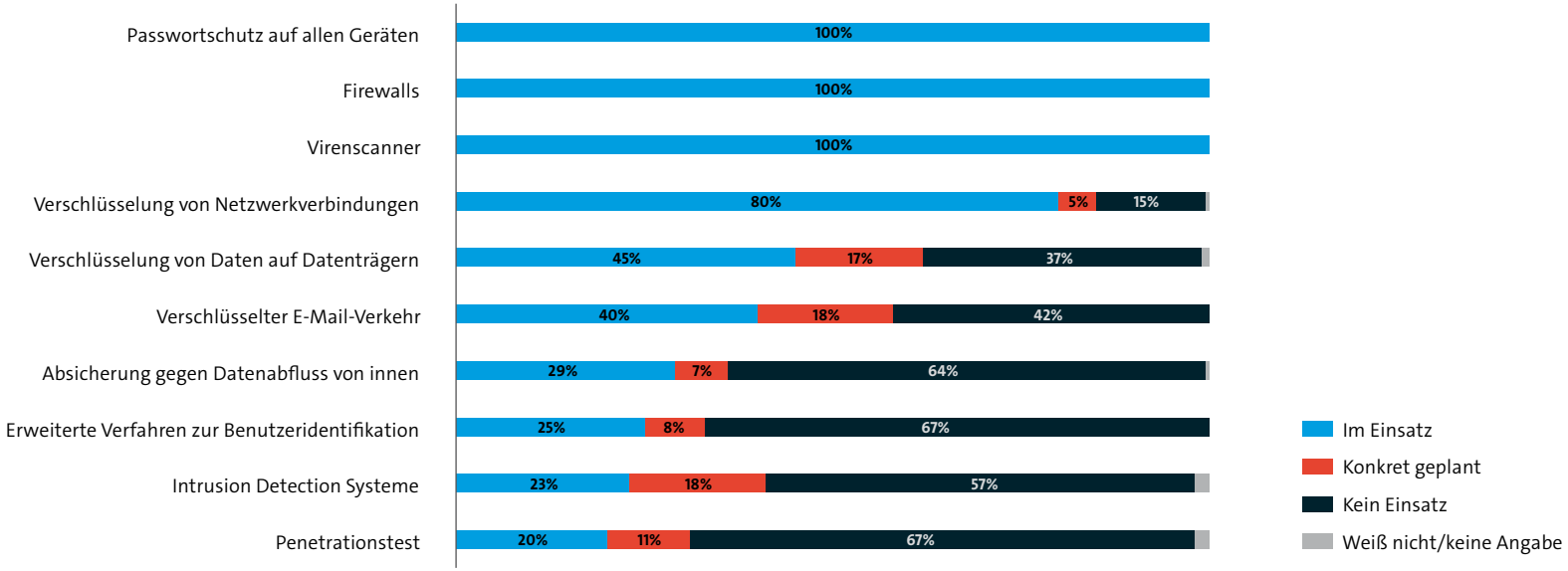
Immerhin vier von fünf (80 Prozent) Unternehmen verschlüsseln zudem ihre Netzwerkverbindungen. Dagegen verschlüsselt nicht mal die Hälfte (45 Prozent) Daten auf Festplatten oder anderen Datenträgern. Nur 40 Prozent setzen auf eine Verschlüsselung ihres E-Mail-Verkehrs.

Nur 29 Prozent der befragten Unternehmen verfügen über eine Absicherung gegen Datenabfluss von innen (Data Leakage Prevention) und nicht einmal ein Viertel (23 Prozent) über spezielle Systeme zur Einbruchserkennung (Intrusion Detection). Diese Anwendungen analysieren die Datenströme in einer Organisation und melden verdächtige Aktivitäten. Sie kommen vor allem dann zum Tragen, wenn Firewall und Virenscanner den Angriff nicht stoppen konnten.

Jedes vierte (25 Prozent) Unternehmen setzt erweiterte Verfahren zur Benutzeridentifikation ein, zum Beispiel eine Zwei-Faktor-Authentifizierung oder biometrische Merkmale. Ein Fünftel der Unternehmen testet die eigenen Sicherheitskonzepte mit Hilfe so genannter Penetrationstests, bei der Angriffe simuliert werden.

Abbildung 16: Eingesetzte technische IT-Sicherheitsmaßnahmen

Basis: Alle befragten Unternehmen (n=1.074)
Quelle: Bitkom Research



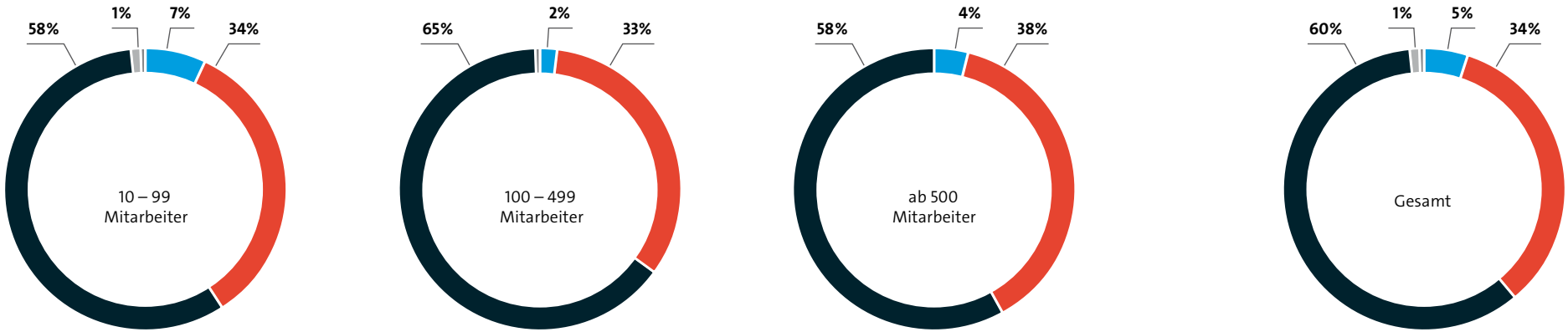
5.4 Die Mehrheit der Befragten sieht Sicherheitsdefizite

Wie sehen sich die Unternehmen selbst gerüstet, um den Gefahren zu begegnen? Immerhin 39 Prozent der Befragten halten das eigene Unternehmen als ausreichend vorbereitet, um Fälle von Datendiebstahl, Sabotage oder Spionage frühzeitig erkennen zu können. Allerdings sieht sich mit 60 Prozent eine deutliche Mehrheit als nicht ausreichend gewappnet an. Nur geringe Unterschiede gibt es hier zwischen den verschiedenen Unternehmensgrößen.

Diese selbstkritische Analyse sollte sich in zusätzlichen Sicherheitsmaßnahmen niederschlagen. Dazu ist einerseits eine Sicherheitskultur notwendig, die alle Unternehmensteile sensibilisiert und damit viele Risiken minimiert. Aber auch Investitionen sind notwendig, um den weiter bestehenden Risiken adäquat begegnen zu können.

Abbildung 17: Einschätzung zur frühzeitigen Erkennung von Vorfällen

Basis: Alle befragten Unternehmen (n=1.074)
Quelle: Bitkom Research



6 Fazit und Empfehlungen

Was sind die Konsequenzen aus den Ergebnissen der Studie?
Drei Aspekte sind von zentraler Bedeutung.

Erstens: Die Unternehmen müssen sich noch stärker und schneller auf die geänderten Bedingungen einstellen. Technische Sicherheitsmaßnahmen alleine reichen nicht aus. Daneben müssen organisatorische und personelle Vorkehrungen getroffen werden. Entscheidend ist zudem, sich auf den Ernstfall vorzubereiten und Pläne zu entwickeln, wie das Ausmaß der Schäden gering gehalten werden kann. Denn einen absoluten Schutz gibt es nicht.

Zweitens: Die Vertrauensbasis zwischen staatlichen Stellen und den Unternehmen ist nur unzureichend entwickelt. Hier muss von beiden Seiten mehr Engagement gezeigt werden. Nur gemeinsam sind die immer komplexeren Herausforderungen zu meistern. Wichtig ist dabei, die Vorteile für beide Seiten stärker herauszuarbeiten.

Und drittens: Beim Thema Unternehmenssicherheit müssen die Mitarbeiter mit einbezogen werden. Nur mit einem höheren Bewusstsein für Sicherheitsaspekte und gezielte Präventionsmaßnahmen kann der Schutz eines Unternehmens verbessert werden.

6.1 Unternehmen müssen Sicherheitsbehörden stärker vertrauen

Das Vertrauen in die deutschen Sicherheitsbehörden ist nicht besonders stark ausgeprägt. Nur 20 Prozent der befragten Unternehmen melden Fälle von Datendiebstahl, Industriespionage oder Sabotage an staatliche Stellen. Als Gründe nennen sie unter anderem Angst vor negativen Auswirkungen, zu hoher Aufwand, geringe Chancen der Aufklärung und Inkompetenz der Sicherheitsbehörden.

Diese Sorgen sind weitgehend unbegründet. Die Sicherheitsbehörden sind fachlich gut aufgestellt und überwiegend gut ausgestattet. Auch sind sie an der Anzeige von Straftaten und einem vertrauensvollen Umgang mit den Informationen interessiert. In der Praxis sind die Behörden sogar abhängig von den Angaben der Betroffenen, um wirkungsvoll arbeiten zu können. Treten zum Beispiel bestimmte Delikte gehäuft auf, fügen sich erst die Informationen mehrerer Geschädigter zu einem Gesamtbild und tragen so zur Aufklärung der Fälle bei. Die Unternehmen helfen sich selbst am meisten, wenn sie Vorfälle zügig an staatliche Stellen weitergeben.

Auf der anderen Seite müssen sich die Sicherheitsbehörden auf Wirtschaft und Bevölkerung zubewegen. Ein positives Beispiel sind die »Zentralen Ansprechstellen Cybercrime« (ZAC) der Landeskriminalämter. Diese Kontaktstellen stehen im Fall der Fälle den betroffenen Unternehmen als helfender Partner zur Verfügung.

Generell brauchen wir mehr Kooperationsbereitschaft auf beiden Seiten. Diese Kooperationen müssen einer gemeinsamen Sache dienen: dem besseren Schutz der deutschen Wirtschaft. Für Unternehmen könnte hier nicht nur das eigene Sicherheitsbedürfnis ein Ansatz sein, sondern auch die Corporate Social Responsibility (CSR). Die Sicherheitsbehörden wiederum sollten nach Transparenz und Vertrauen streben. Bitkom arbeitet derzeit in zwei sehr erfolgreichen Kooperationen mit staatlichen Sicherheitsbehörden zusammen: mit verschiedenen Landeskriminalämtern in der »Sicherheitskooperation Cybercrime« und mit dem BSI in der »Allianz für Cybersicherheit«. Auch einzelne Unternehmen können der Allianz beitreten oder sich direkt an die Landeskriminalämter wenden.

Grundsätzlich brauchen wir weitere Kooperationen und eine intensivere Zusammenarbeit in den bestehenden Initiativen, denn nur durch die Zusammenarbeit von staatlichen Behörden und der Wirtschaft im Bereich des Wissenstransfers, der Prävention und der Steigerung des Bewusstseins lässt sich das immer komplexer werdende Feld der digitalen Sicherheit bewältigen.

6.2 Umdenken bei der Informationssicherheit: Schadensbegrenzung ergänzt Prävention

Lange galten Firewalls und Virenscanner als das Maß der Dinge, wenn es darum ging, Unternehmen vor Hackerangriffen zu schützen. Diese Zeiten sind vorbei. Da die Bedrohungen immer vielfältiger und die IT-Infrastrukturen immer komplexer werden, reicht ein rein präventiver Ansatz zum Schutz der Unternehmensinformationen nicht mehr aus: Ein Unternehmen muss lernen, mit Sicherheitsvorfällen professionell umzugehen und den entstandenen Schaden zu minimieren. Das so genannte »Incident Management« bzw. IT-Störungsmanagement ergänzt die bisherigen Schutzkonzepte.

Der wesentliche Grund für das Umdenken ist die aktuelle Bedrohungslage. Angriffe durch kriminelle Hacker nehmen zu. Die Angriffe werden ausgefeilter, komplexer und spezifischer. Gleichzeitig nimmt die Asynchronität zwischen Angriff und Verteidigung zu: Der Angreifer muss nur ein Schlupfloch finden, die Sicherheitsverantwortlichen aber eine Vielzahl von Systemen mit noch mehr potentiellen Schwachstellen absichern. Angriffe werden arbeitsteilig und in kriminellen Strukturen organisiert und als Dienstleistung mit Support über das Internet zu günstigen Konditionen angeboten. Die Zunahme der so genannten APT-Angriffe (advanced persistent threats) zeigt, dass es für Angreifer möglich ist, sich über Jahre unerkannt in den IT-Infrastrukturen der Unternehmen zu bewegen. Das alles geschieht vor dem Hintergrund, dass die IT-Systeme immer leistungsfähiger werden und die Anzahl der potenziell gefährdeten Endgeräte im Zuge der Digitalisierung beständig zunimmt.

Der Fokus liegt deshalb zunehmend auf der Erkennung von Einbrüchen, um wie im Fall von komplexen APT-Angriffen Schadensbegrenzung betreiben zu können. Der Ausbau der Sensorik im Unternehmensnetz – im Sinne der Erkennung von Anomalien – steht also im Fokus der Sicherheitsbemühungen. In diesem Zusammenhang kommen vermehrt Angriffserkennungssysteme (intrusion detection) zum Einsatz. Diese Systeme analysieren die Datenströme in einer Organisation und melden verdächtige Aktivitäten. Sie können die Schwächen eines rein reaktiven Ansatzes mindern und sehr schnell Hinweise auf einen möglichen Sicherheitsvorfall liefern. Um die Daten der Sensorik auszuwerten, müssen Unternehmen ihre IT-Abteilungen aufstocken - finanziell, aber auch personell.

Der Ansatz zum Incident-Management darf nicht auf die Erkennung eines Angriffes beschränkt bleiben. Notwendig sind Maßnahmen zur Analyse und Beendigung des Angriffes, zur Wiederherstellung des Betriebszustandes, zur Datenwiederherstellung sowie zur Bewertung von Schäden. Dabei sollten externe Partner wie die Polizei, der Verfassungsschutz, IT-Sicherheitsdienstleister oder IT-Forensiker frühzeitig einbezogen werden. Nicht zuletzt müssen Organisationen das Verhalten im Notfall zum Beispiel in Form eines Planspiels einüben. Die Maßnahmen reichen vom Stopfen eines Datenlecks über die Information aller wichtigen Personen und der Medien bis zum Neustart des Geschäftsbetriebs.

6.3 Organisatorische, physische und personelle Sicherheit – Hinweise für Mitarbeiter

Die Sicherheit in der digitalen Welt beschränkt sich nicht auf rein technische Maßnahmen der IT-Sicherheit. Sie müssen durch organisatorische und physische Maßnahmen ergänzt werden. Dazu gehören unter anderem Regelungen, wer im internen Netzwerk auf welche Daten zugreifen darf und wer Zutritt zu sensiblen Bereichen eines Unternehmens bekommt. Letztere müssen durch entsprechende Zugangskontrollen für Mitarbeiter, Dienstleister oder Gäste gewährleistet werden. Voraussetzung dafür ist, dass das Betriebsgelände und die Gebäude geschützt werden können. Andernfalls müssen bauliche Maßnahmen ergriffen werden.

Zentraler Sicherheitsfaktor sind die Mitarbeiter. Nur etwa die Hälfte der befragten Unternehmen führt Schulungen der Beschäftigten oder Sicherheitsüberprüfungen von Bewerbern durch. Eine angemessene Sicherheitskultur umfasst darüber hinaus die richtige Verwendung von Zugangsdaten, den korrekten Umgang mit externen Datenträgern oder Verhaltensregeln auf Reisen. Der Bitkom gibt einige praktische Hinweise, wie Mitarbeiter die Sicherheit des Unternehmens gewährleisten können.

Der Mitarbeiter als wirkungsvollste »Firewall«

Jeder Mitarbeiter im Unternehmen kann wesentlich zur Sicherheit des Unternehmens beitragen. Dazu gehört die konsequente Umsetzung der Sicherheitsvorgaben, aber auch eine gewisse Aufmerksamkeit und Sensibilität für verdächtige Situationen. Befinden sich zum Beispiel nicht angemeldete Personen im Haus oder in der Abteilung, sind Türen oder Fenster defekt oder parkt neuerdings ein Kleinbus neben der WLAN-Antenne?

Aber nicht nur im analogen Leben gibt es Betrugsversuche, die schnell zu einer Gefahr für die Unternehmenssicherheit werden können. Falsche Rechnungen von imaginären Lieferanten oder Buchungsbestätigungen nicht existierender Reisebüros gehören in deutschen Unternehmen zum Alltag. Unternehmen müssen ihre Mitarbeiter immer wieder zu einem kritischen Umgang mit scheinbar banalen Situationen und Informationen ermutigen. Dann liegt es an dem Anwender, hier wachsam zu sein und mögliche Gefahren zu erkennen. Jetzt braucht es nur noch den Mut, die Geschehnisse zu melden, zu prüfen und Maßnahmen daraus abzuleiten. Der Mitarbeiter ist die wirkungsvollste »Firewall« eines Unternehmens und kann nicht durch technische Geräte ersetzt werden.

Social Engineering – eine verbreitete Gefahr

Viele der Vorfälle im Bereich Wirtschaftsschutz werden von den eigenen Mitarbeitern verursacht, oftmals nicht aus krimineller Energie heraus, sondern durch Unvorsichtigkeit und Unbedarftheit. Ein beliebtes Mittel, um in abgeschlossene Netzwerke zu gelangen, sind geschenkte USB-Sticks. Nicht selten befindet sich ein Schadprogramm darauf.

Ein anderes Beispiel ist eine empfangene E-Mail, verbunden mit einem Anruf von einer externen Rufnummer, welcher sich als ein Vorgesetzter ausgibt und hektisch die Bearbeitung einer angehängten Datei verlangt. Auch hier liegt ein Schadprogramm dahinter. In beiden Fällen heißt es, lieber einmal mehr nachgedacht oder nachgefragt. Hektik und Neugier sind hier zwei schlechte Berater, die womöglich zu einem erheblichen Schaden für die Firma führen können.

Kommunikation im öffentlichen Raum

Auf Reisen im Zug, auf dem Bahnhof oder auf dem Flughafen wird die Zeit gerne genutzt, um E-Mails zu schreiben oder wichtige Telefonate zu führen. Dabei wird oftmals vergessen, dass man sich im öffentlichen Raum bewegt und potenziell Interessierte nicht viel mehr machen müssen, als Augen und Ohren offen zu halten.
Deshalb sollten Telefonate, die sich auf keinen Fall verschieben lassen, in ruhigeren Abschnitten des Bahnhofs oder Flughafens geführt werden, und zwar mit gedämpfter Lautstärke. Das gleiche gilt für Telefonate im Zug. Zudem sollte der Laptop oder das Tablet mit einer Sichtschutzfolie ausgestattet werden. Diese verhindert ein seitliches Einsehen auf den Bildschirm und die darauf dargestellten Inhalte.

Akten und Unterlagen richtig entsorgen

Selbst beim Ausmisten der Büros sollten Mitarbeiter achtsam sein. Anstatt alles einfach in der blauen Tonne zu entsorgen, sollten Unterlagen aus dem Büroumfeld mittels Aktenvernichter zerkleinert und erst danach entsorgt werden. Unbeschädigt weggeworfene Dokumente sind für Kriminelle, aber auch die Konkurrenz ein willkommener Fundus zur Informationsgewinnung.

Methode

Viele deutsche Unternehmen sind aufgrund ihrer innovativen Produkte und ihrer starken Position auf den Weltmärkten ein lukratives Ziel für kriminelle Hacker und ausländische Geheimdienste. Der Diebstahl sensibler Unternehmensdaten, der Ausfall von IT-Systemen oder eine Unterbrechung der Produktion als Folge digitaler Angriffe verursachen Schäden in Milliardenhöhe. Mit der vorliegenden Studie untersucht der Digitalverband Bitkom, welche Unternehmen von entsprechenden Vorfällen betroffen sind, wer die mutmaßlichen Täter sind und ob sich die Wirtschaft ausreichend schützt. Außerdem wurde auch die Höhe der verursachten Schäden ermittelt. Ein besonderes Augenmerk wurde dabei auf die Betreiber kritischer Infrastrukturen, die für die Versorgung der Gesellschaft von besonderer Bedeutung sind, gelegt.

Dafür wurden insgesamt 1.074 nach Branchen und Größenklassen repräsentativ ausgewählte Unternehmen mit mindestens zehn Mitarbeitern befragt. Es handelt sich um die bislang umfassendste empirische Untersuchung dieses Themas in Deutschland. Die Interviews wurden mit Führungskräften durchgeführt, die in ihrem Unternehmen für das Thema Wirtschaftsschutz verantwortlich sind. Dazu zählen Geschäftsführer sowie Führungskräfte aus den Bereichen Unternehmenssicherheit, IT-Sicherheit, Risikomanagement oder Finanzen.

Durch Schichtung der Zufallsstichprobe wurde dabei gewährleistet, dass Unternehmen aus den unterschiedlichen Branchen und Größenklassen in für statistische Auswertungen ausreichender Anzahl vertreten sind. Die Aussagen der Befragungsteilnehmer wurden bei der Analyse gewichtet, so dass die Ergebnisse ein nach Branchengruppen und Größenklassen repräsentatives Bild für alle Unternehmen ab zehn Mitarbeitern in Deutschland ergeben.

Mit der konkreten Durchführung der computergestützten telefonischen Interviews (CATI) wurde das Marktforschungsinstitut Aris Umfrageforschung mbH in Hamburg beauftragt. Die Interviews wurden von im Vorfeld speziell geschulten Telefoninterviewern im Januar und Februar 2015 realisiert. Der standardisierte Fragebogen wurde von der Bitkom Research GmbH in Zusammenarbeit mit dem Digitalverband Bitkom konzipiert.